

**TRANSMITTAL OF APPEAL BRIEF**Docket No.
00-VE04.75B CIPIn re Application of: Arthur Duskow *et al.*Application No.
09/767,292Filing Date
January 18, 2001Examiner
P.W. KlimachGroup Art Unit
2135

Invention: METHOD OF AND APPARATUS FOR AUTHENTICATING CONTROL MESSAGES IN A SIGNALING NETWORK

TO THE COMMISSIONER OF PATENTS:Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: May 2, 2007The fee for filing this Appeal Brief is \$ 500.00☒ Large Entity ☐ Small Entity☒ A petition for extension of time is also enclosed.The fee for the extension of time is \$ 120.00☒ A check in the amount of \$ 620.00 is enclosed.☐ Charge the amount of the fee to Deposit Account No. 06-2375
This sheet is submitted in duplicate.☐ Payment by credit card. Form PTO-2038 is attached.☒ The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 06-2375
This sheet is submitted in duplicate.Dated: August 2, 2007Michael J. Strauss
Attorney Reg. No. : 32,443
FULBRIGHT & JAWORSKI L.L.P.
801 Pennsylvania Avenue, N.W.
Washington, DC 20004-2623
(202) 662-4632**Appeal Brief Transmittal**

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being hand delivered on the date shown below to: Customer Window, MS Appeal Brief - Patents, U.S. Patent and Trademark Office, Randolph Building, 401 Dulany Street, Alexandria, Virginia 22314.

Dated: August 2, 2007

Signature: _____ (Michael J. Strauss)



Docket No.: 00-VE04.75B CIP
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Arthur Duskow et al.

Application No.: 09/767,292

Confirmation No.: 9811

Filed: January 18, 2001

Art Unit: 2135

For: METHOD OF AND APPARATUS FOR
AUTHENTICATING CONTROL MESSAGES
IN A SIGNALING NETWORK

Examiner: P. W. Klimach

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under § 41.37(a), this brief is filed more than two months after the Notice of Appeal filed in this case on May 2, 2007, and is in furtherance of said Notice of Appeal.

The fees required under § 41.20(b)(2) are dealt with in the accompanying
TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R.
§ 41.37 and M.P.E.P. § 1205.2.

08/03/2007 HLE333 00000097 09767292

01 FC:1402

500.00 0P



TABLE OF CONTENTS

I.	REAL PARTY IN INTEREST.....	1
II.	RELATED APPEALS AND INTERFERENCES.....	2
III.	STATUS OF THE CLAIMS.....	3
IV.	STATUS OF AMENDMENTS.....	4
V.	SUMMARY OF CLAIMED SUBJECT MATTER	5
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL.....	7
VII.	ARGUMENT	9
A.	Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” In View of Bissell and Further In View of Vince.....	10
1.	Claim 1	10
a.	<i>Control Messages</i>	10
b.	<i>Chronologically Sequenced</i>	13
2.	Dependent Claims 5 and 6 are Separately Patentable	15
3.	Dependent Claim 7 is Separately Patentable	15
4.	Dependent Claim 10 is Separately Patentable	16
5.	Dependent Claims 14 - 15 are Separately Patentable.....	16
6.	Dependent Claim 16 is Separately Patentable	17
7.	Dependent Claim 17 is Separately Patentable	17
B.	Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” In View of Bissell and Further In View of Vince and Further in View of Sawyer	18
C.	Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” In View of Bissell and Further In View of Vince and Further in View of Arkko	18
D.	Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” in view of Bissell and further in view of Vince and further in view of Hanson	18
1.	Dependent Claim 18 is Separately Patentable	19
2.	Dependent Claim 19 is Separately Patentable	19
3.	Dependent Claim 20 is Separately Patentable	20
4.	Dependent Claim 18 is Separately Patentable	20
5.	Dependent Claims 22 – 24 are Separately Patentable	21
E.	Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” In View Of Sawyer and Further In View Of Vince	22
1.	Claim 25	22

a.	<i>Chronological Sequencing</i>	22
2.	Dependent Claims 31 - 32 Are Separately Patentable.....	24
F.	Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” in view of Sawyer and further in view of Vince and further in view of Bissell	24
1.	Dependent Claim 34 Is Separately Patentable.....	24
2.	Dependent Claim 39 Is Separately Patentable.....	25
3.	Dependent Claim 40 Is Separately Patentable.....	25
G.	Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” in view of Sawyer and further in view of Vince and further in view of Hanson	25
1.	Dependent Claim 35 Is Separately Patentable.....	25
2.	Dependent Claim 36 Is Separately Patentable.....	26
3.	Dependent Claim 37 Is Separately Patentable.....	27
4.	Dependent Claim 38 Is Separately Patentable.....	27
H.	Rejection of Claim 33 is Improper	28
I.	Conclusion	28
VIII.	CLAIMS APPENDIX.....	30
IX.	EVIDENCE APPENDIX	38
X.	RELATED PROCEEDINGS APPENDIX.....	39



I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Verizon Services Corp., an affiliate of Verizon Communications Inc., with offices located at One Verizon Way, Basking Ridge, NJ 07920.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 40 claims pending in application.

B. Current Status of Claims

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1 – 40.
4. Claims allowed: None
5. Claims rejected: 1 - 40¹

C. Claims On Appeal

The claims on appeal are claims 1- 40.

¹ The “Office Action Summary” for the Final Office Action lists claims 1-40 as rejected, however the Examiner did not set forth a rejection of claim 33 in the Detailed Action. To advance prosecution of this application, Applicant includes claim 33 in this appeal due to this ambiguity.

IV. STATUS OF AMENDMENTS

Applicant did not file an Amendment After Final Rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A summary of the claimed subject matter with cross-reference to elements of the preferred embodiments described in the specification is provided below. Such cross-reference is not a representation by applicant that the scope of the claimed subject matter be limited to the preferred embodiments.

According to claim 1, a communication network (e.g., fig. 1, 110) comprises (A) local communication links (e.g., fig. 1, 120 and 122), (B) a plurality of separately located central office switching systems (e.g., fig. 1, 112 and 114), (C) a signaling communication system (e.g., fig. 1, 130 including 136, 138, 140, 142, 144, 146, 148, 152, 156, 158, 160, and 174), (D) a signaling gateway (e.g., fig. 1, 170), and (E) a signaling system security monitor (e.g., fig. 1, 150 or 154). The plurality of separately located central office switching systems (112 and 114) are interconnected via trunk circuits (116 and 118) for selectively providing switched call connections between at least two of the local communication links (120 and 122) in response to predetermined control data messages (e.g., page 4, lines 23 – 25; page 39, line 1 – page 41, line 19; and, e.g., MTP, SCCP, TCAP and/or ISUP messages of figs. 8 - 12). Signaling communication system (130) provides two-way communications of the control data messages (figs 8 - 12) between the central office switching systems (112 and 114) with, the signaling communication system (130) being interconnecting the central office switching systems (112 and 114, e.g., via 136 and 138, respectively). Signaling gateway (170) is separate from central office switching systems (112 and 114) and is connected to the signaling communications system (130). The signaling gateway (170) includes an interface (e.g., fig. 1, 172) connected to a remote communications network (e.g., fig. 1, 200) and is configured to exchange the control data messages (figs. 8 - 12) between the remote communication network (200) and the central office switching systems (114, 116) by way of the signaling communication system (130). Signaling system security monitor (150 or 154) is separate from the central office switching systems (112 and 114) and is configured to evaluate an encrypted portion of the control data messages (figs. 8 - 12) including digital time stamps (page 41, lines 20 -22) so as to authenticate corresponding ones of the control messages and, in response, determine if the control data messages are chronologically sequenced (e.g., page 12, lines 22 – 24; page 40, lines 18 – 19).

According to claim 25 a method of securely interfacing control links of respective communication networks comprises the steps of (i) exchanging control data messages (e.g., figs. 8 - 12) between a remote communication network (200) and a local signaling communication system (130) (e.g., page 39, lines 1 – 8); (ii) decrypting a certificate portion of the control messages including a time stamp so as to authenticate origination originating point code information based on the time stamp so as to determine control message timeliness and chronological sequencing (e.g., page 13, lines 11 -13; page 39, line 8 – page 40, line 2 (iii) selectively communicating, in response to the decrypting step, control data messages (e.g., figs. 8 - 12) between central office switching systems (112 and 114) (e.g., page 40, lines 3 – 24); and (iv) selectively providing switched call connections between at least two of the local communication links in response to predetermined control data messages (e.g., figs. 8 – 12)(e.g., page 15, lines 3 – 11 and page 40, lines 24 - 26).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Applicant seeks review of the following grounds of rejection set forth in the Final Office Action having a notification date of February 2, 2007 (hereinafter the "Office Action"):

A. Whether claims 1 and 5 – 17 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over applicant's admitted prior art in view of U.S. Patent No. 6,574,730 (filed February 11, 1997, issued June 3, 2003) to Bissell et al. (hereinafter "Bissell") and further in view of U.S. Patent No. 4,562,539 (filed February 17, 1983, issued December 31, 1985) to Vince (hereinafter "Vince").

B. Whether claims 2 and 3 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over applicant's admitted prior art in view of Bissell and further in view of Vince and further in view of U.S. Patent No. 6,324,271 to Sawyer (hereinafter "Sawyer").

C. Whether claim 4 is properly rejected under 35 U.S.C. § 103(a) as being unpatentable over applicant's admitted prior art in view of Bissell and further in view of Vince and further in view of U.S. Patent Publication No. 20020052200 to Arkko et al. (hereinafter "Arkko").

D. Whether claims 18 – 24 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over applicant's admitted prior art in view of Bissell and further in view of Vince and further in view of U.S. Patent No. 6,014,427 (filed December 26, 1996, issued January 11, 2000) to Hanson et al. (hereinafter "Hanson").

E. Whether claims 25 - 32 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over applicant's admitted prior art in view of Sawyer and further in view of Vince.

F. Whether claims 34, 39 - 40 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over applicant's admitted prior art in view of Sawyer and further in view of Vince and further in view of Bissell.

G. Whether claims 35 - 38 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over applicant's admitted prior art in view of Sawyer and further in view of Vince and further in view of Hanson.

H. Whether claim 33 is properly rejected.

VII. ARGUMENT

As more fully set forth below, the rejections by the Examiner in the Office Action are improper because:

1. The Examiner improperly ignores the meaning of “control messages” according to Applicant’s claims taking the position that user signaling for controlling access is equivalent to control messages exchanged among network elements in performing network functions.
2. The Examiner improperly ignores the meaning of “chronologically sequenced” according to Applicant’s claims taking the position that a teaching of detecting an ordering is equivalent.
3. The dependent claims include limitations not taught or suggested by the references cited by the Examiner.

Applicant’s invention is directed to “systems and call processing methodologies that analyze signaling traffic to identify, correct and/or reject inappropriate, invalid and/or harmful messages.” Other than Applicant’s description of the background of the invention, the remaining art cited by the Examiner fails to recognize or address a problem of moderating interconnections between signaling networks. At most, the cited prior art describes limiting access to a network by confirming the identify of a user or user terminal attempting such access. Given a fair reading, the cited prior art has little if anything to do with call processing within or between communications networks. In spite to these defects, the Examiner has attempted to cobble together a hodgepodge of teachings in formulating the outstanding rejections, which amount to an impermissible hindsight reconstruction of the invention using the claims as a template.

Applicant addresses each of the grounds of rejection below.

A. Rejections under 35 U.S.C. §103 Based on the “Admitted Prior Art” In View of Bissell and Further In View Of Vince

The undersigned initially notes that the rejection as presented on page 2 of the Office Action misrepresents the combination of art applied against the rejected claims, the narrative further including reference to Schneier, presumably as applied in the prior Office Action of May 31, 2006 at page 4. However, as the Examiner has failed to clearly indicate reliance on Schneier as part of the rejection as stated, while acknowledging the failure of the asserted combination to teach the claimed invention (see, e.g., Office Action at page 3, final paragraph), the rejection is improper.

1. Claim 1

a) *“Control Data Messages”*

The Examiner improperly ignores the meaning of “control messages” according to Applicant’s claims, taking the position that signals used for controlling access to a network are equivalent to those used within a network to perform network functions. Claim 1 requires:

...central office switching systems...selectively providing switched call connections ... in response to predetermined control data messages,

...a signaling gateway...configured to exchange said control data messages between said remote communication network and said central office switching systems ..., and

...a signaling system security monitor...configured to evaluate an encrypted portion of said control data messages including digital time stamps so as to authenticate corresponding ones of said control messages and, in response, determine if said control data messages are chronologically sequenced.

The specification describes that these control messages as follows:

SS7 is a standard established and maintained by the American National Standards Institute (ANSI) defining procedures and protocols used by network elements of PSTNs to exchange data for call setup, routing and control (e.g., ISUP messages) and for the exchange of non-circuit related information between signaling points (e.g., transactional TCAP messages). SS7 messages are transmitted between network elements, known as signaling points (SP) using 56 or 64 kbps bidirectional channels called signaling links. SPs include Service Switching Points (SSPs), Signal Transfer Points (STPs), and Service Control Points (SCPs). SSPs are the switches that originate, terminate, or route (i.e., “tandem”) calls. SCPs provide centralized databases and support other centralized call processing functions required by special services (e.g., 800 numbers, enhanced call forwarding services, etc.) SCPs may be queried by an SSP using TCAP to obtain call routing and call handling information. The STPs route these network **control messages** over the SS7 network between and among the SSPs and SCPs as necessary.

Page 4, line 23 – page 5, line 5;

The claimed “control messages” are not merely generalized signals but are messages used by a network to “selectively [provide] switched call connections.” Applicants teach including in these control messages an encrypted portion including digital time stamps that are used by a security monitor to determine if the control messages are chronologically sequenced. Applicants do not merely claim a signal used to authenticate a user or control access to a network. Applicants claim incorporates specific features into a control messages used by the network to provide switched call connections between network switching systems.

In the Office Action, the Examiner relies on Bissell for evaluating an encrypted portion of an authentication code which the Examiner appears to consider as equivalent to “a control data message”; it is not. Bissell’s authentication code has nothing to do with establishing switched call connections between network switching systems, only to providing network access to a subscriber terminal. It is not equivalent to the claimed control data messages. Further, Bissell never suggests authenticating a **message** as required by Claim 1, but only authentication of a user **terminal**.

Bissell is directed to **user** authentication in a communications network (see, e.g., title of the invention):

An authentication system of a terminal on a public switched telephone network provides a security node associated with a local exchange and a network terminal.

... [A] match between expected and received authentication codes constitutes authentication of the terminal allowing the user access to the network.

Bissell, Abstract of the Disclosure.

Bissell uses encryption to provide network access to a terminal, NOT to authenticate a control message used to provide switched call connections between central office switching systems. Note, for example, Figure 4 showing the Bissell “authentication” process beginning with a customer “Off Hook” action and ending with a response from the security device to provide that user with either restricted or normal service. While Bissell may authenticate a user (or, more properly, a user terminal) attempting to place a call, the claimed invention authenticates the control messages exchanged between switching systems as an attempt is made to setup a call within the network. The two are not equivalent.

Not only does Bissell fail to describe or suggest authentication of a control message for the reasons presented above, but the teaching of Bissell are inappropriate for use within a network. In part this is due to the specific call initiation method as taught by Bissell. In particular, call initiation according to Bissell comprises a two step process. First, the caller (or more properly, the caller’s terminal) is authenticated then, secondly, the caller is permitted to place a call. The disclosure proposes no authentication, and no security is provided beyond the original challenge and response that establishes that the caller’s terminal is entitled to place a call. The signal sent from the network terminating equipment to the security node does not include any information about the call to be placed. It is only once the user’s equipment is validated that the user is permitted to make calls. For a validated user Bissell does not propose the capability to restrict which calls can be placed.

In contrast, applicant’s network includes structure that authenticates the actual control messages themselves. These are the messages that are passed between network elements and are involved in setting up and tearing down calls between them. They are also involved in maintaining the network. This is far different from Bissell which only provides protection against unauthorized end users (or more accurately, users of unauthorized end user terminals),

but does nothing about the possibility of the introduction or detection of unauthorized control messages within call handling network.

b) *“Chronologically Sequenced”*

The Examiner improperly ignores the meaning of “chronologically sequenced” according to Applicant’s claims, claim 1 additionally requiring such a determination be made with regard to an encrypted time stamp. In the Office Action, the Examiner takes the position that a teaching of detecting an ordering is equivalent. Detecting an order of messages is NOT the same as determining the chronology of messages.

Admitting that Bissell fails to teach use of digital time stamps to determine that control data messages are properly sequenced, the Examiner applies Vince. However, not only is the Vince disclosure directed to non-analogous art, but it fails to teach or suggest determining if messages are chronologically sequenced based on encrypted time stamp information. Vince is directed to ensuring that all messages are received in the same sequence by a multiplicity of terminals and that messages present in an output queue are processed prior to accepting update messages from other nodes that would update a local database. There is no discussion of the use of time stamps to determine if control data messages are chronologically sequenced. Nor does Bissell assert that transmitted messages are ordered in the sequence that they were generated (as they would be, were they chronologically sequenced).

The Examiner relies on the following portion of Vince as teaching that messages are chronologically sequenced:

If the node receives an update message from another node while it (the first node) still has at least one outstanding update message, the received message may overwrite the data item which has already been updated by the first node at the time it created the outstanding message. The data item would thus be overwritten by a chronologically earlier value, and this is clearly incorrect. **(It will be recalled that the chronology of the updates is determined by the order in which the update messages are received from the link).** This situation is detected by the AND gate 29, which receives the inverses of the signals CZ and TN. The output of the gate 29 sets a bistable 32 producing a signal SUSP (suspend) which causes the processor 14 to suspend its operation. The processor then remains suspended until the counter 24 returns to zero, indicating that all

outstanding messages have been received. The signal CZ then resets the bistable 32, removing the suspension.

Vince at column 5, lines 29 – 46, emphasis added.

As indicated by the language shown in bold above, Vince equates chronology of the updates to be the **order** in which the messages are received from the link, not the time at which the message was generated. In contrast, Claim 1 requires evaluation of an encrypted portion of a control data message, including digital time stamps, so as to authenticate the control messages and determine if the control data messages are chronologically sequenced. While the Vince specification uses the term “chronology”, the specification makes clear that it means order, not the time at which the message was created.

Vince is directed to update messages transmitted by processing nodes connected to a token ring network. The patent is directed to the problem of messages being received out of order due to message latency while awaiting transmission onto the ring. Vince addresses this problem by inhibiting updates to a local memory until a particular node has an opportunity to transmit its own memory update message. Thus, although Vince states that it prevents overwriting of a data item “by a chronologically earlier value”, the term “chronologically earlier” refers to an order in which messages were placed on a bus, rather than to a time at which the message was generated. To the contrary, Vince has no way to determine when a message is generated as it does not associate or time stamp the messages as required by Claim 1.

Although not mentioned in the formal recitation of the rejection of claims 1 and 5 – 17 appearing at page 2 of the Office Action, recognizing that Vince fails to suggest the use of time stamps, the Examiner further relies on Schneier in the narrative explanation (Office Action at page 4). That is, the Examiner takes the position that Schneier describes that which is lacking in the combination of the admitted prior art in view of Bissell and further in view of Vince. However, Schneier describes signing documents and, as part of creating a digital signature, including a time stamps to avoid a repeat attack. There is no mention of using the time stamp in any other environment than in signing documents and, certainly, not in connection with

determining if messages are chronologically sequenced, only whether the message is a duplicate. Thus, even adding the teachings of Schneier fails to render obvious the subject matter of claim 1.

2. Dependent Claims 5 and 6 Are Separately Patentable

Claim 5 requires that the signaling system security monitor selectively communicate the control data message between the signaling gateway and the signaling communication system in response to the encrypted portion of the control data messages. Claim 6 requires that the signaling system security monitor selectively enable and inhibit said signaling gateway from exchanging control data messages between a remote communication network and the signaling communication system in response to encrypted portions of the control data messages. According to the Examiner, Bissell teaches such an arrangement. However, Bissell does not teach selectively communicating a control data message, only permitting a user terminal to connect to a network. That is, Bissell's control signal is always communicated to the security node so as to enable or disallow dialing of the terminal. Similarly, Bissell fails to teach selectively enabling and inhibiting the exchange of control data messages. Further Bissell fails to describe exercising control over such a control data message within a network such as between a signaling gateway and a signaling communication system.

3. Dependent Claim 7 Is Separately Patentable

Contrary to the Examiner's position, Bissell simply fails to describe or suggest storing states of each of the central office switching systems and using those stored states to determine if control messages are proper. Bissell states only that:

The operation of a telephony service may be modelled [sic.] in terms of a sequence of states a call may go through. These states, and the relationship between states, form what is termed a 'call model'. Analysis of the call model reveals that there are a number of opportunities for introducing an authentication attempt.

Bissell at column 8, lines 9 – 14.

However, Bissell fails to describe or suggest storing such state information or using it to determine if control messages are proper.

4. Dependent Claim 10 Is Separately Patentable

It is noted that the Examiner's rejection appears to be based on a version of Claim 10 prior to the most recent amendment. However, it is nonetheless improper for the failure of Bissell to teach or suggest monitoring of a destination point code. While Bissell may monitor a dialed telephone number, a destination point code is a specific term of art, providing the routable address of a network element, not mere dialed digits constituting a telephone number:

Using SS7, the signaling system security monitor is configured to monitor information contained in an MTP Layer 3 portion of the control data messages. The information monitored may include (i) a destination point code, (ii) an originating point code, and/or (iii) a service indicator.

Specification at page 14, lines 2 – 5.

Bissell describes only that, if authorization is not successful, the customer may be permitted to dial certain allowed telephone numbers. However, there is no reference to monitoring a **destination point code** as required by claim 10.

5. Dependent Claims 14 and 15 Are Separately Patentable

Claims 14 and 15 require that the said signaling system security monitor be configured to monitor origination and destination point codes contained in a TCAP message portion of the control data messages. The cited portion of Bissell only describes monitoring a dialed telephone number to permit limited calling if authorization is denied. There is no description in Bissell of

monitoring origination and destination point codes or any other portion of a TCAP message portion of a control data message; there is no mention of TCAP at all.

6. Dependent Claim 16 Is Separately Patentable

The Examiner appears to take the position that recognizing an off-hook condition is equivalent to storing a state of the network instantiation of a call. However, monitoring for an off-hook condition is, at most, monitoring a state of a terminal that is attempting to connect to the network, not a state of the network itself. Secondly, while the Examiner takes the position that “[t]he states would have to be stored for the authentication process to know what to send next”, there is no support cited for this conclusion. Further, these are states of the call initiation and termination, not states of the network element implementation of the call.

7. Dependent Claim 17 Is Separately Patentable

Claim 17 requires that the signaling system security monitor include a memory storing permissible states of the communications network and rules for transitioning from each of said permissible states to others of the permissible states. The Examiner again equates an off-hook condition of a terminal to the claimed permissible states of the communications network; they are not. The Examiner further assumes that the states would be stored without citing any support. The Examiner still further takes the position that “[t]he steps taken for authentication to be positive imply the rules for transition from one state to another.” Again, Bissell is silent on storing permissible states or what transitions are permissible.

B. Rejections under 35 U.S.C. §103 Based on the “Admitted Prior Art” In View of Bissell and Further In View Of Vince and Further in View of Sawyer

Claims 2 and 3 each depend from Claim 1, and therefore are patentable over the combination of the admitted prior art, Bissell and Vince references applied by the Examiner, for at least the same reasons as claim 1. The Examiner’s inclusion of Sawyer does not correct the deficiencies of the combined admitted prior art, Bissell and Vince references noted above with respect to claim 1, and therefore claims 2 and 3 are patentable over the Examiner’s cited combination.

C. Rejections under 35 U.S.C. §103 Based on the “Admitted Prior Art” In View of Bissell and Further In View Of Vince and further in view of Arkko.

Claim 4 depends from Claim 1, and therefore is patentable over the combination of the admitted prior art, Bissell and Vince references applied by the Examiner, for at least the same reasons as claim 1. The Examiner’s inclusion of Arkko does not correct the deficiencies of the combined admitted prior art, Bissell and Vince references noted above with respect to claim 1, and therefore claim 4 is patentable over the Examiner’s cited combination.

D. Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” in view of Bissell and further in view of Vince and further in view of Hanson

In connection with claims 18 – 24, as each is dependent from Claim 1, each requires that the signaling system security monitor evaluate an encrypted portion of a control data messages including digital time stamps so as to authenticate corresponding ones of the control messages and, in response, determine if the control data messages are chronologically sequenced. None of the references as applied in the rejection of claims 18 – 24 mention use of such a time stamp. Accordingly, the rejection of claims 18 – 24 is improper.

1. Dependent Claim 18 Is Separately Patentable

The Examiner asserts that Figure 4 depicts a voice mail messaging system that stores messages depending the progress of a call. However, Figure 4 is described by Hanson as “a flowchart illustrating the creation of an action message using a telephone interface...” (Brief Description of the Drawing at column 2, lines 26 – 27.) At most, the flowchart depict various steps performed by a voice mail system. In contrast, claim 18 requires that signaling system security monitor include a memory storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service. Call progress as used in Claim 18 refers to processing for establishing, conducting, maintaining and tearing-down a voice connection. Hanson is silent on such and, as such, does not render the subject matter of claim 18 obvious.

2. Dependent Claim 19 Is Separately Patentable

The Examiner asserts that Figure 4A, block 406 discloses a system wherein the user can store a plurality of message templates. The applicable text of Hanson describes that:

The action message script generator 226 prompts the message creator to indicate the desired number of pre-defined responses that will be offered to the voice message recipient as shown in block 406. In this illustrative example of the invention, a number between 1-9 is indicated using the telephone keypad as shown in block 408.

Hanson at column 4, lines 28 – 33.

The Examiner’s reliance on block 408 for showing or otherwise describing a template is misplaced. While Hanson does describe the use of templates, these are for facilitating voice message creation: that bear no relation to approved control data messages used to control switches:

For example, to minimize complexity for the message creator, a limited number of action message "templates" may be pre-programmed and offered to the message creator from a template menu.

Column 5, lines 9 – 12.

3. Dependent Claim 20 Is Separately Patentable

Claim 20, dependent upon claim 19, further requires that plurality of message templates be associated with a plurality of service providers. The Examiner takes the position that "the messages disclosed by Hanson are dependent on the user and therefore the user may refer to a plurality of service providers, wherein each provider is represented by a prompt." Office Action at page 12. Even if the user "may" refer to a service provider, Hanson never describes or suggests as much. To the contrary, the disclosure never refers to "service providers", nor is it understood why Hanson would refer to having templates associated with service providers. "Messages" and "templates" as used by Hanson bear no relation to "messages" and "templates" as described in this application, either in their form or usage.

4. Dependent Claim 21 Is Separately Patentable

Claim 21, dependent from claim 20, requires that the signaling system security monitor associate each of the control data messages with a corresponding one of the service providers and selects one of the message templates in response to the corresponding one of the service providers. The Examiner states that "the action messages allow the user to relate a prompt with a message; therefore each service provider would correspond to a message and the caller would chose a prompt as shown in Hanson for the action to be taken." Office Action at page 12.

As previously explained, appellant's control data messages are different from those of the applied art such the language of clam 21 is not satisfied. The applied art also fails to describe or

suggest associating templates with service providers.. Further, the rationale presented by the Examiner fails to explain or identify any portion of Hanson supporting the contention that Hanson describes associating control data messages with corresponding service providers or selecting a template in response to the corresponding service provider.

5. Dependent Claims 22 – 24 Are Separately Patentable

Claim 22, and thereby claims 23 – 24 dependent therefrom, require the signaling system security monitor include a memory storing sets of templates, each of said sets corresponding to control messages appropriate to particular call progress flow. The Examiner takes the position that:

Hanson discloses a voice mail messaging system wherein the system stores messages on the progress of the call (Fig. 4). The user can prompt the caller so as to initiate a next action, the action would lead to the service associated with the prompt (column 4 lines 40 -50). The progress of the call would correspond to the progress flow.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to relate cal [sic.] progress status with the respective sets of control messages as in Hanson in the system of applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because the user would be allowed to custom the message on the system.

Office Action at page 13.

To the extent understood, the Examiner still fails to explain how Hanson describes of suggests storing a set of templates, each set corresponding to control messages appropriate to a particular call progress flow. Further, even if the prior art did describe as much, the Examiner has failed to provide a viable argument for why one skilled in the art would be motivated to combine elements of a communications network as per the admitted prior art with the user authentication system of Bissell, the data processing system of Vince and the voice mail system according to Hanson to produce the asserted combination.

E. Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” In View Of Sawyer and Further In View Of Vince

1. Claim 25

The rejection of claim 25 is improper for the reasons presented above in connection with claim 1 and as set forth below.

a) *Chronological Sequencing*

The Examiner again improperly ignores the meaning of “chronological sequencing” according to Applicant’s claims and specification (claim 25 requiring such a determination be made with regard to a decrypted time stamp), taking the position that a teaching of detecting an ordering is equivalent. Detecting an order of messages is NOT the same as determining chronological control message chronological sequencing as claimed.

Admitting that Sawyer fails to teach that a control data message is chronologically sequenced, the Examiner applies Vince. However, the Vince disclosure fails to teach or suggest determining if messages are chronologically sequenced based on decrypted time stamps information. Vince is directed to ensuring that messages present in an output queue are processed prior to accepting update messages from other nodes that would update a local database. There is no discussion of the use of time stamps to determine if control data messages are chronologically sequenced, nor does Vince’s description of the message format allow for the inclusion of any information that would permit chronological sequencing.

The Examiner relies on the following portion of Vince as teaching that messages are chronologically sequenced:

If the node receives an update message from another node while it (the first node) still has at least one outstanding update message, the received message may overwrite the data item which has already been updated by the first node at the time it created the outstanding message. The data item would thus be overwritten by a chronologically earlier value, and this is clearly incorrect. (It

will be recalled that the chronology of the updates is determined by the order in which the update messages are received from the link). This situation is detected by the AND gate 29, which receives the inverses of the signals CZ and TN. The output of the gate 29 sets a bistable 32 producing a signal SUSP (suspend) which causes the processor 14 to suspend its operation. The processor then remains suspended until the counter 24 returns to zero, indicating that all outstanding messages have been received. The signal CZ then resets the bistable 32, removing the suspension.

Vince at column 5, lines 29 – 46, emphasis added.

As indicated by the language shown in bold above, Vince equates chronology of the updates to be the **order** in which the messages are received from a link, not the time at which the message was generated. The prospect of contention for the token ring on which Vince is based eliminates any possibility that the order in which messages are received from the link could be construed as being the chronological order in which they were generated. In contrast, Claim 25 requires determining if a control message is **chronologically sequenced** based on a decrypted portion of a control message, including a time stamp, so as to authenticate the control messages. While the Vince specification uses the term “chronology”, the specification makes clear that it means order, not the time that the message was created.

Vince is directed to update messages transmitted by processing nodes connected to a token ring network. The patent is directed to the problem of messages being received out of order due to message latency while awaiting transmission onto a token-ring network. Vince addresses this problem by inhibiting updates to a local memory until a particular node has an opportunity to transmit its own memory update message. Thus, although Vince states that it prevents overwriting of a data item “by a chronologically earlier value”, the term “chronologically earlier” refers to an order of messages rather than to a time at which the message was generated. To the contrary, Vince has no way to determine when a message is generated as it does not associate or time stamp the messages as required by Claim 25.

Although not mentioned in the formal recitation of the rejection of claims 25 - 32, recognizing that Vince fails to suggest the use of time stamps, the Examiner again takes the position that Schneier describes that which is lacking in the combination of the admitted prior art

in view of Bissell and further in view of Vince. Schneier describes signing documents and, as part of creating a digital signature, including a time stamps to avoid a repeat attack. However there is no mention of using the time stamp in any other environment than in signing documents and, certainly, not in connection with determining if messages are chronologically sequenced, only if the message is a duplicate. Thus, even adding the teachings of Schneier fails to render obvious the subject matter of claim 25.

2. Dependent Claims 31 and 32 Are Separately Patentable

It is initially noted that, while the recitation of the rejection of claims 25 – 32 appearing at the bottom of page 13 of the Office Action relies on the combination of the admitted prior art in view of Sawyer and further in view of Vince, the narrative rejection of claims 31 and 32 appearing at page 16 of the Office Action instead applies Bissell. It further appears that narrative addressing subject claims 31 and 32 appearing at page 16, line 3 – page 17, line 5 is substantively identical with that presented in connection with claims 14 and 15 at page 7, lines 8 – page 8, line 9 (e.g., refers to and parrots the language of claims 14 and 15 rather than that to the language of subject claims 31 and 32). As the rejection fails to address the actual language of claims 31 and 32, it is believed improper. Further, to the extent the Examiner intends to apply such art against claims 31 and 32, the rejections are further improper for the reasons set forth *supra* in connection with claims 14 and 15, which arguments for patentability are incorporated herein by reference.

F. Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art,” In View of Sawyer and further in view of Vince and further in view of Bissell

1. Dependent Claim 34 Is Separately Patentable

Claim 34 requires a step of storing (i) permissible states of the communications network and (ii) rules for transitioning from each of the permissible states to others of the permissible

states. As in connection with claim 17, the Examiner again equates an off-hook condition of a terminal to the claimed permissible states of the communications network; they are not. The Examiner further assumes that the states would be stored without citing any support. Bissell is silent on storing permissible states or what transitions are permissible. Thus, the language of claim 34 is not satisfied by the asserted combination.

2. Dependent Claim 39 Is Separately Patentable

The Examiner asserts that Sawyer at column 8, lines 26 – 50, teaches monitoring of an originating point code. No such disclosure can be found. Originating Point Code is a term of art with specific meaning not found in Sawyer. Thus, claim 39 is not rendered obvious.

3. Dependent Claim 40 Is Separately Patentable

The Examiner asserts that Sawyer at column 8, lines 26 – 50, teaches monitoring of a service indicator.. No such disclosure can be found. Service Indicator is a term of art with specific meaning not found in Sawyer. Thus, claim 40 is not rendered obvious.

G. Rejections Under 35 U.S.C. § 103 Based on “Admitted Prior Art” in view of Sawyer and further in view of Vince and further in view of Hanson

1. Dependent Claim 35 Is Separately Patentable

As with claim 18, the Examiner asserts that Figure 4 depicts a voice mail messaging system that stores messages depending the progress of a call. However, Figure 4 is described by Hanson as “a flowchart illustrating the creation of an action message using a telephone interface...” At most, the flowchart depict various steps performed by a voice mail system. In

contrast, claim 18 requires that signaling system security monitor include a memory storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service. Call progress as used in Claim 18 refers to processing to establish, conduct, maintain and tear-down a voice connection. Hanson is silent on such and, as such, does not render the subject matter of claim 18 obvious.

2. Dependent Claim 36 Is Separately Patentable

As with claim 16, the Examiner asserts that Figure 4A, block 406 discloses a system wherein the user can store a plurality of message templates. The applicable text of Hanson describes that:

The action message script generator 226 prompts the message creator to indicate the desired number of pre-defined responses that will be offered to the voice message recipient as shown in block 406. In this illustrative example of the invention, a number between 1-9 is indicated using the telephone keypad as shown in block 408.

Hanson at column 4, lines 28 – 33.

The Examiner's reliance on block 408 for showing or otherwise describing a template is misplaced. While Hanson does describe the use of templates, these are for voice message creation, not corresponding to approved control data messages used to control switches:

For example, to minimize complexity for the message creator, a limited number of action message "templates" may be pre-programmed and offered to the message creator from a template menu.

Column 5, lines 9 – 12.

3. Dependent Claim 37 Is Separately Patentable

As with claim 20, the Examiner again takes the position that “the messages disclosed by Hanson are dependent on the user and therefore the user may refer to a plurality of service providers, wherein each provider is represented by a prompt.” Office Action at page 19. Even if the user “may” refer to a service provider, Hanson never describes or suggests as much. To the contrary, the disclosure never refers to “service providers”. Nor is it understood why Hanson would refer to having templates associated with service providers. Thus, the rejection of claim 37 is improper.

4. Dependent Claim 38 Is Separately Patentable

Paralleling claim 21, claim 38, dependent from claim 37, requires associating each of the control data messages with a corresponding one of the service providers and selecting one of the message templates in response to the corresponding one of the service providers. The Examiner states that “the action messages allow the user to relate a prompt with a message; therefore each service provider would correspond to a message and the caller would chose a prompt as shown in Hanson for the action to be taken.” Office Action at page 19.

As previously explained, appellant’s control data messages are different than those of the applied art. Further, the rationale presented by the Examiner fails to explain or identify any portion of Hanson supporting the contention that Hanson describes associating control data messages with corresponding service providers or selecting a template in response to the corresponding service provider.

H. Claim 33 is Improperly Rejected

Claim 33 was indicated as rejected on the Office Action Summary for the Office Action, but no rejection of claim 33 is provided in the Detailed Action. To the extent the Examiner intended to reject claim 33, such a rejection is improper, for example, under 37 C.F.R. § 1.105(c)(2):

In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. *The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified.* (emphasis added)

Applicant thus seeks reversal of the rejection of claim 33.

I. Conclusion

Appellant has provided arguments that overcome the pending obviousness rejections. The Examiner's conclusion that the claims should be rejected is unwarranted. Therefore, Appellant respectfully requests that the Board overturn the Examiner's rejection of claims 1-40.

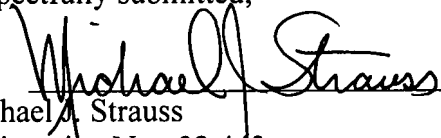
A copy of the claims involved in the present appeal is attached hereto as Appendix A. As indicated above, the claims in Appendix A include the amendments filed by Applicant on October 30, 2006.

This Appeal Brief is accompanied by payment of the fee for filing a brief in support of an appeal under 41.20(b)(2) together with a petition and corresponding fee for a one month extension of time. If any additional fees are due in connection with this filing, please charge our Deposit Account No. 08-2025, under Order No. 414.038CIP/10007256 from which the undersigned is authorized to draw and please credit any excess fees to such deposit account.

Dated: August 2, 2007

Respectfully submitted,

By


Michael A. Strauss

Registration No.: 32,443

FULBRIGHT & JAWORSKI L.L.P.

801 Pennsylvania Avenue, N.W.

Washington, DC 20004-2623

(202) 662-0200

(202) 662-4643 (Fax)

Attorney for Applicant

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/767,292

1. A communication network, comprising:
 - (A) local communication links,
 - (B) a plurality of separately located central office switching systems interconnected via trunk circuits for selectively providing switched call connections between at least two of the local communication links in response to predetermined control data messages,
 - (C) a signaling communication system for two-way communications of said control data messages between said central office switching systems, said signaling communication system interconnecting the central office switching systems;
 - (D) a signaling gateway, separate from the central office switching systems and connected to said signaling communications system, said signaling gateway including an interface connected to a remote communications network and configured to exchange said control data messages between said remote communication network and said central office switching systems by way of said signaling communication system, and
 - (E) a signaling system security monitor, separate from the central office switching systems, said signaling system security monitor configured to evaluate an encrypted portion of said control data messages including digital time stamps so as to authenticate corresponding ones of said control messages and, in response, determine if said control data messages are chronologically sequenced.

2. The communications network according to claim 1 wherein said signaling system security monitor comprises a certification agent configured to exchange and maintain encryption key certificates.
3. The communications network according to claim 1 wherein said signaling system security monitor is configured to issue and decrypt said digital time stamps.
4. The communications network according to claim 1 wherein said signaling system security monitor comprises a digital certificate issuing authority.
5. The communications network according to claim 1 wherein said signaling system security monitor is configured to selectively communicate said control data messages between said signaling gateway and said signaling communication system in response to said encrypted portions of said control data messages.
6. The communications network according to claim 1 wherein said signaling system security monitor is configured to selectively enable and inhibit said signaling gateway from exchanging said control data messages between said remote communication network and said signaling communication system in response to said encrypted portions of said control data messages.
7. The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing states of respective ones of said central office switching systems, said processor additionally responsive to said states for determining if said control messages are proper.

8. The communications network according to claim 1 wherein said signaling gateway is configured to convert SS7 type messages to another packet data format.
9. The communications network according to claim 8 wherein the other packet data format is an Internet Protocol (IP) format.
10. The communications network according to claim 1 wherein said signaling system security monitor is configured to monitor.
11. The communications network according to claim 1 wherein said signaling system security monitor is configured to monitor at least one of SCCP, ISUP, TCAP, and AIN messages.
12. The communications network according to claim 1 wherein said signaling system security monitor is configured to monitor calling and called party address parameters contained in SCCP message portions of said control data messages and determine if said monitor calling and called party address parameters are consistent with an authorized signaling relationship.
13. The communications network according to claim 1 wherein said signaling system security monitor is configured to monitor calling and called party address parameters contained in an SCCP message portion of said control data messages.
14. The communications network according to claim 1 wherein said signaling system security monitor is configured to monitor origination and designation point codes and calling and called party address parameters contained in a TCAP message portion of said control data messages.

15. The communications network according to claim 1 wherein said signaling system security monitor is configured to monitor origination and destination point codes parameters contained in a TCAP message portion of said control data messages and determine if a particular destination point code is authorized to send a particular TCAP message to a particular destination point code.
16. The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing a state of said communications network.
17. The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing permissible states of said communications network and rules for transitioning from each of said permissible states to others of said permissible states.
18. The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.
19. The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing a plurality of message templates corresponding to approved ones of said control data messages.
20. The communications network according to claim 19 wherein said plurality of message templates are associated with a plurality of service providers..

21. The communications network according to claim 20 wherein said signaling system security monitor associates each of said control data messages with a corresponding one of said service providers and selects one of said message templates in response to the corresponding one of said service providers.
22. The communications network according to claim 19 wherein said signaling system security monitor includes a memory storing sets of templates, each of said sets corresponding to control messages appropriate to particular call progress flow.
23. The communications network according to claim 22 wherein said templates define message formats, parameters and values associated with control message types selected from SCCP, ISUP, TCAP and AIN type messages.
24. The communications network according to claim 22 wherein said signaling system security monitor is configured to select said sets of templates in response to service provider authorization data associated with respective ones of said control data messages.
25. A method of securely interfacing control links of respective communication networks, comprising the steps of:
 - exchanging control data messages between a remote communication network and a local signaling communication system;
 - decrypting a certificate portion of said control messages including a time stamp so as to authenticate originating point code information based on said time stamp so as to determine control message chronological sequencing;

selectively communicating, in response to said decrypting step, control data messages between central office switching systems; and

selectively providing switched call connections between at least two of the local communication links in response to predetermined control data messages.

26. The method according to claim 25 further comprising a step of converting a protocol of said control data messages between a protocol of said remote communication network and a protocol of said local signaling communication system.
27. The method according to claim 26 wherein one of said protocols is an SS7 compliant message protocol.
28. The method according to claim 27 wherein one of said protocols is an Internet Protocol (IP) format.
29. The method according to claim 25 further comprising a step of monitoring of calling and called party address parameters contained in SCCP message portions of said control data messages.
30. The method according to claim 29 wherein said monitoring step includes determining if said calling and called party address parameters are consistent with an authorized signaling relationship.
31. The method according to claim 25 further comprising a step of monitoring origination and designation point codes and calling and called party address parameters contained in a TCAP message portion of said control data messages.

32. The method according to claim 31 wherein said monitoring step includes monitoring origination and destination point codes parameters contained in a TCAP message portion of said control data messages and determining if a particular destination point code is authorized to send a particular TCAP message to a particular destination point code.
33. The method according to claim 25 further comprising a step of storing a state of said communications network.
34. The method according to claim 25 further comprising a step of storing (i) permissible states of said communications network and (ii) rules for transitioning from each of said permissible states to others of said permissible states..
35. The method according to claim 25 further comprising a step of storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.
36. The method according to claim 25 further comprising a step of storing a plurality of message templates.
37. The method according to claim 36 wherein said plurality of message templates are associated with a plurality of service providers.
38. The method according to claim 37 further comprising steps of:

associating each of said control data messages with a corresponding one of said service providers; and

selecting one of said message templates in response to the corresponding one of said service providers.

39. The communications network according to claim 1 wherein said signaling system security monitor is configured to monitor an originating point code.
40. The communications network according to claim 1 wherein said signaling system security monitor is configured to monitor a service indicator.

APPENDIX B

EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

APPENDIX C
RELATED PROCEEDINGS

No related proceedings are referenced in II. above, hence copies of decisions in related proceedings are not provided.